

EVALUACIÓN FINAL

PRUEBA DE HABILIDADES CCNP

CAMILO ANDRES CAMARGO OLIVEROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

INGENIERIA DE TELECOMUNICACIONES

DIPLOMADO CISCO CCNP

TUNJA

2019

PRUEBA DE HABILIDADES CCNP

CAMILO ANDRES CAMARGO OLIVEROS

Diplomado de profundización cisco CCNP prueba de Habilidades prácticas

Gerardo Granados Acuña
Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
INGENIERIA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP

TUNJA
2019

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Tunja 08 de septiembre de 2019

GLOSARIO

CISCO: Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CCNP: Cisco Certified Network Professional es uno de los niveles del plan de capacitación en tecnología de redes informáticas que la empresa Cisco ofrece.

NETWORKING: Es la integración de dos sistemas de redes completas. Una red consiste en dos o más computadoras unidas que comparten recursos.

PROTOCOLO: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

INTERFAZ: Una interfaz de red es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.

ROUTING: Es el proceso de determinar el mejor camino para realizar el encaminamiento. En otras palabras, Routing es el proceso que se realiza para determinar las tablas de encaminamiento.

SWITCHING: Son dispositivos de propósito específico diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.

OSPF: Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

BGP: es un protocolo de gateway exterior (EGP), usado para realizar el ruteo entre dominios en las redes TCP/IP.

EIGRP: es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace.

VLAN: Virtual LAN (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física.

VTP: VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

PROTOCOLO IP Es la base fundamental de la Internet. Porta datagramas de la fuente al destino. El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino.

GNS3: Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios, imágenes IOS de CiscoSystems.

RESUMEN

En este documento están solucionados los escenarios propuestos para la prueba de las habilidades del Diplomado de profundización de cisco CCNP, se muestra paso a paso la configuración de los routers y switches con los protocolos IPv4 e IPv6, y los protocolos de Routing y Switching según el escenario. Se anexan también, las imágenes con los resultados de los comandos ping, traceroute, show ip route, entre otros, dependiendo de los requerimientos para cada caso. El escenario 1 consiste en realizar la configuración de OSPF y EIGRP; El escenario 2 consiste en realizar la configuración de EIGRP; El escenario 3 consiste en realizar la configuración de VLANs y VTP en una red de Switches.

Palabras clave: cisco, ccnp, networking, protocolo, router, switch, Routing, Switching, ospf, ebgp, eigrp, vlan, vtp, dtp, IPv4, IPv6.

ABSTRACT

In this document is the solution of the scenarios proposed for the Cisco CCNP skills test, the configuration of the routers and switches with the IPv4 and IPv6 protocols, and the Routing and Switching protocols according to the scenario are shown step by step.

The images with the results of the ping, traceroute, show ip route commands, among others, are also attached, depending on the requirements for each case. Scenario 1 consists of performing the OSPF and EIGRP configuration; Scenario 2 consists of performing the EIGRP configuration; Scenario 3 consists of configuring VLANs and VTP in a network of switches.

Keywords: Cisco, ccnp, networking, protocol, router, switch, Routing, Switching, ospf, ebgp, eigrp, vlan, vtp, dtp, IPv4, IPv6.

CONTENIDO

INTRODUCCIÓN	11
ESCENARIO 1	12
Configuración de interfaces y Ospf en R1.....	13
Configuración de interfaces y Ospf en R2.....	13
Configuración de interfaces y Ospf en R3.....	14
Configuración de interfaces y Ospf en R4.....	15
Configuración de interfaces y Ospf en R5.....	15
Configuración de interfaces loopback en R1	16
Configuración de interfaces loopback en R5.....	18
Redistribución de rutas EIGRP en OSPF R3	20
ESCENARIO 2	23
Configuración interfaces y loopback R1	24
Configuración interfaces y loopback R2.....	25
Configuración interfaces y loopback R3.....	25
Configuración interfaces y loopback R4.....	26
Configuración de BGP neighbor AS2 en R1	27
Configuración de BGP neighbor AS1 en R2	27
Configuración de BGP neighbor AS3 en R2	27
Configuración de BGP neighbor y AS2 y 1 en R3.....	28
Configuración de BGP neighbor y AS4 en R3.....	28
Configuración de BGP neighbor y AS3 en R4.....	28
ESCENARIO 3	33
Configuración VTP en SW1.	33
Configuración VTP en SW2.	34
Configuración VTP en SW3.	34
Configuración troncal dinámico en SW1.	35

Configuración troncal dinámico en SW2.	35
Configuración de Interfaces en SW1.....	36
Configuración de Interfaces en SW3.....	36
Configuración de Interfaces en SW2.....	37
Configuración de Interfaces en SW3.....	37
Configuración de vlans en SW1	38
Configuración de vlans en SW2	38
Configuración de VLANs en SWT1.	40
Configuración de VLANs en SWT2.....	40
Configuración de VLANs en SWT3	40
Configuración de F0/10 en SWT1.	41
Configuración de F0/10 en SWT2.	41
Configuración de F0/10 en SWT3.	41
Configuración de F0/15 y F0/20 en SWT1.	42
Configuración de F0/15 y F0/20 en SWT2.	42
Configuración de F0/15 y F0/20 en SWT3.	43
Configuración en STW1.	43
Configuración en STW2.	44
Configuración en STW3.	45
 CONCLUSIONES	 48
 REFERENCIAS	 49

LISTA DE TABLAS

Tabla 1 Interfaces Loopback en R1	16
Tabla 2 Interfaces Loopback en R5	17
Tabla 3 Configuración inicial Escenario 2	24
Tabla 4 Interfaces, VLANs e IP	39
Tabla 5 Direcciones SVI VLAN99	43

LISTA DE FIGURAS

Figura 1 Topología Escenario 1	12
Figura 2 Tabla de enrutamiento R3	19
Figura 3 Tabla de enrutamiento R3	20
Figura 4 Tabla de enrutamiento R1	21
Figura 5 Tabla de enrutamiento R5	22
Figura 6 Topología Escenario 2	23
Figura 7 Tabla de enrutamiento R1	29
Figura 8 Tabla de enrutamiento R2	30
Figura 9 Tabla de enrutamiento R3	31
Figura 10 Tabla de enrutamiento R4	32
Figura 11 Topología Escenario 3	33
Figura 12 VTP Status.....	34
Figura 13 Trunk SWT1 y SWT2.....	36
Figura 14 Trunk SWT1 y SWT3.....	37
Figura 15 VLANs en SWT1 y SWT2.....	39
Figura 16 Pruebas de PING en PCs.....	46
Figura 17 Pruebas de PING en Swithces	46
Figura 18 Pruebas PING entre Switches y PCs.....	47

INTRODUCCIÓN

Gracias al constante crecimiento de las empresas y su competitividad a nivel mundial, las redes de Telecomunicaciones crecen con ellas exigiendo a los profesionales del área, entregar y administrar una infraestructura eficaz y segura, lo que a su vez le exige a los ingenieros, técnicos, gestores de red, estar en la capacidad de afrontar cualquier reto, proporcionar las mejores soluciones para los requerimientos que tiene el área de las Telecomunicaciones hoy en día.

Con el desarrollo de esta prueba de Habilidades Practicas del Diplomado de Profundización CCNP, se busca poner en práctica los conocimientos adquiridos a lo largo del desarrollo de los módulos de Routing y Switching, y aplicarlos en los 3 diferentes escenarios propuestos para esta actividad y poner a prueba diversas habilidades para dar soluciones y cumplir con los objetivos de cada escenario.

ESCENARIO 1

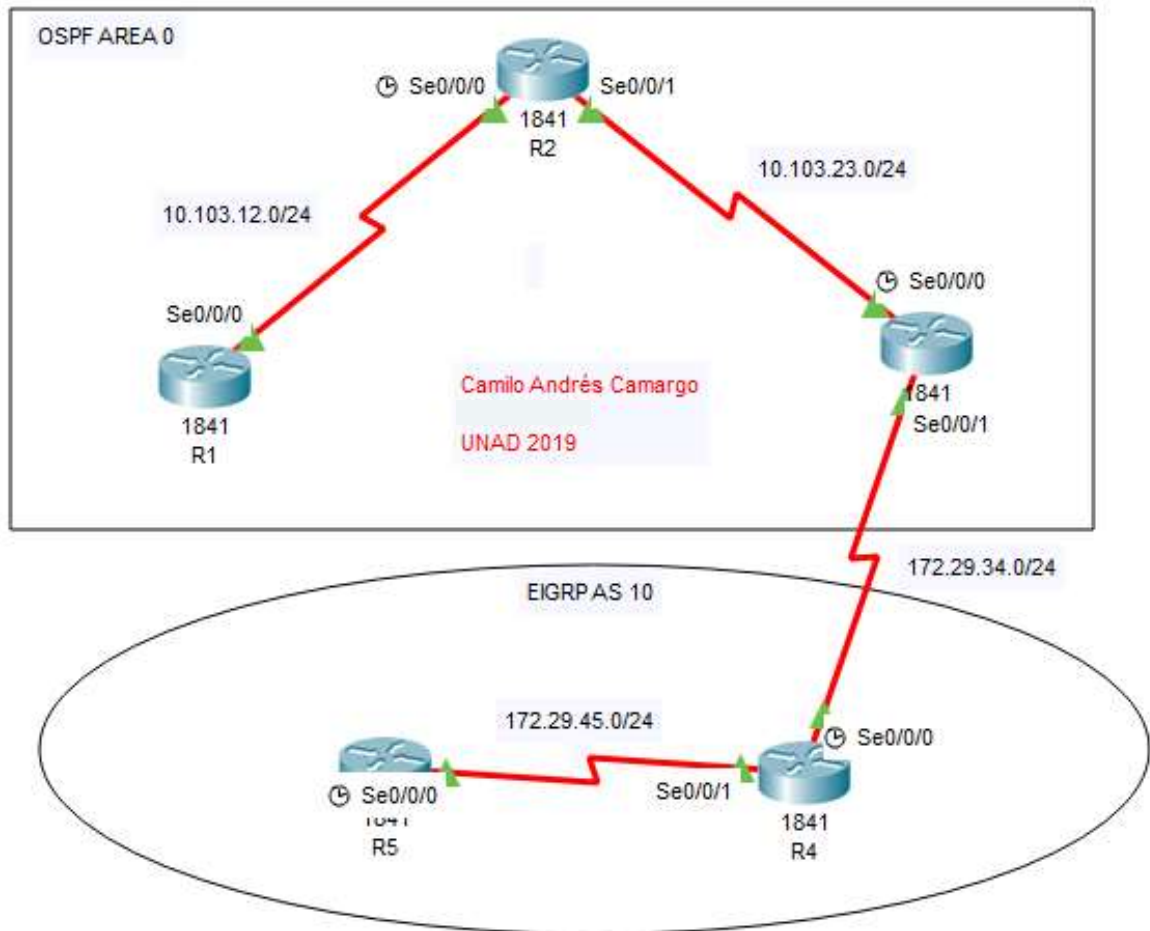


Figura 1 Topología Escenario 1

1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Configuración de interfaces y Ospf en R1.

```
enable
configure terminal
no ip domain-lookup
hostname R1

interface loopback 1

interface serial 0/0/0
ip address 10.103.12.2 255.255.255.0
clock rate 128000
no shutdown
exit

router ospf 1
router-id 1.1.1.1
network 10.1.0.0 0.0.3.255 area 0
network 10.103.12.0 0.0.0.255 area 0
end

copy running-config startup-config
```

Configuración de interfaces y Ospf en R2.

```
enable
configure terminal
no ip domain-lookup
hostname R2

interface loopback 2

interface serial 0/0/0
ip address 10.103.12.1 255.255.255.0
no shutdown
exit

interface serial 0/0/1
ip address 10.103.23.2 255.255.255.0
no shutdown
exit
```

```
router ospf 1
router-id 2.2.2.2
network 10.103.12.0 0.0.0.255 area 0
network 10.103.23.0 0.0.0.255 area 0
end

copy running-config startup-config
```

Configuración de interfaces y Ospf en R3.

```
enable
configure terminal
no ip domain-lookup
hostname R3

interface loopback 3

interface serial 0/0/0
ip address 10.103.23.1 255.255.255.0
clock rate 128000
no shutdown
exit

interface serial 0/0/1
ip address 172.29.34.2 255.255.255.0
no shutdown
exit

router ospf 1
router-id 3.3.3.3
network 10.103.23.0 0.0.0.255 area 0
end

copy running-config startup-config
```

Configuración de interfaces y Ospf en R4.

```
enable
configure terminal
no ip domain-lookup
hostname R4

interface loopback 4

interface serial 0/0/0
ip address 172.29.34.1 255.255.255.0
no shutdown
exit

interface serial 0/0/1
ip address 172.29.45.2 255.255.255.0
no shutdown
end

copy running-config startup-config
```

Configuración de interfaces y Ospf en R5.

```
enable
configure terminal
no ip domain-lookup
hostname R5

interface loopback 5

interface serial 0/0/0
ip address 172.29.45.1 255.255.255.0
clock rate 128000
no shutdown

end

copy running-config startup-config
```

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Interfaces Loopback en R1	
Loopback10	10.1.10.1/22
Loopback20	10.1.20.1/22
Loopback30	10.1.30.1/22
Loopback40	10.1.40.1/22

Tabla 1 Interfaces Loopback en R1

Configuración de interfaces loopback en R1

```
enable
configure terminal

interface loopback10
ip address 10.1.10.1 255.255.252.0
exit.

interface loopback20
ip address 10.1.20.1 255.255.252.0
exit

interface loopback30
ip address 10.1.30.1 255.255.252.0
exit

interface loopback40
ip address 10.1.40.1 255.255.252.0
exit

router ospf 1
router-id 1.1.1.1
```



```

network 10.1.0.0 0.0.3.255 area 0
network 10.103.12.0 0.0.0.255 area 0
exit

interface loopback10
ip ospf network point-to-point
exit

interface loopback20
ip ospf network point-to-point
exit

interface loopback30
ip ospf network point-to-point
exit

interface loopback40
ip ospf network point-to-point
end

copy running-config startup-config

```

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

Interfaces Loopback en R5	
Loopback50	172.5.50.1/22
Loopback60	172.5.60.1/22
Loopback70	172.5.70.1/22
Loopback80	172.5.80.1/22

Tabla 2 Interfaces Loopback en R5

Configuración de interfaces loopback en R5

```
interface loopback510
ip address 172.5.50.1 255.255.252.0
exit
```

```
interface loopback60
ip address 172.5.60.1 255.255.252.0
exit
```

```
interface loopback70
ip address 172.5.70.1 255.255.252.0
exit
```

```
interface loopback80
ip address 172.5.80.1 255.255.252.0
exit
```

```
route eigrp 10
auto-summary
network 172.5.0.0 0.0.3.255
network 172.29.45.0 0.0.0.255
```

4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

```

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.1.0.0/22 [110/129] via 10.103.23.2, 00:04:36,
Serial0/0/0
O       10.103.12.0/24 [110/128] via 10.103.23.2,
4294967274:4294967255:4294967270, Serial0/0/0
C       10.103.23.0/24 is directly connected, Serial0/0/0
      172.29.0.0/24 is subnetted, 1 subnets
C       172.29.34.0 is directly connected, Serial0/0/1
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Figura 2 Tabla de enrutamiento R3

- Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

$$\text{Formula Costo} = \frac{100000}{BW(Kbps)}$$

Redistribución de rutas EIGRP en OSPF R3

```
router ospf 1
 redistribute eigrp 10 metric 50000 subnets
exit
```

Redistribuir las rutas OSPF en EIGRP

```
router eigrp 10
 redistribute ospf 1 metric 100000 20000 255 255 1500
end
```

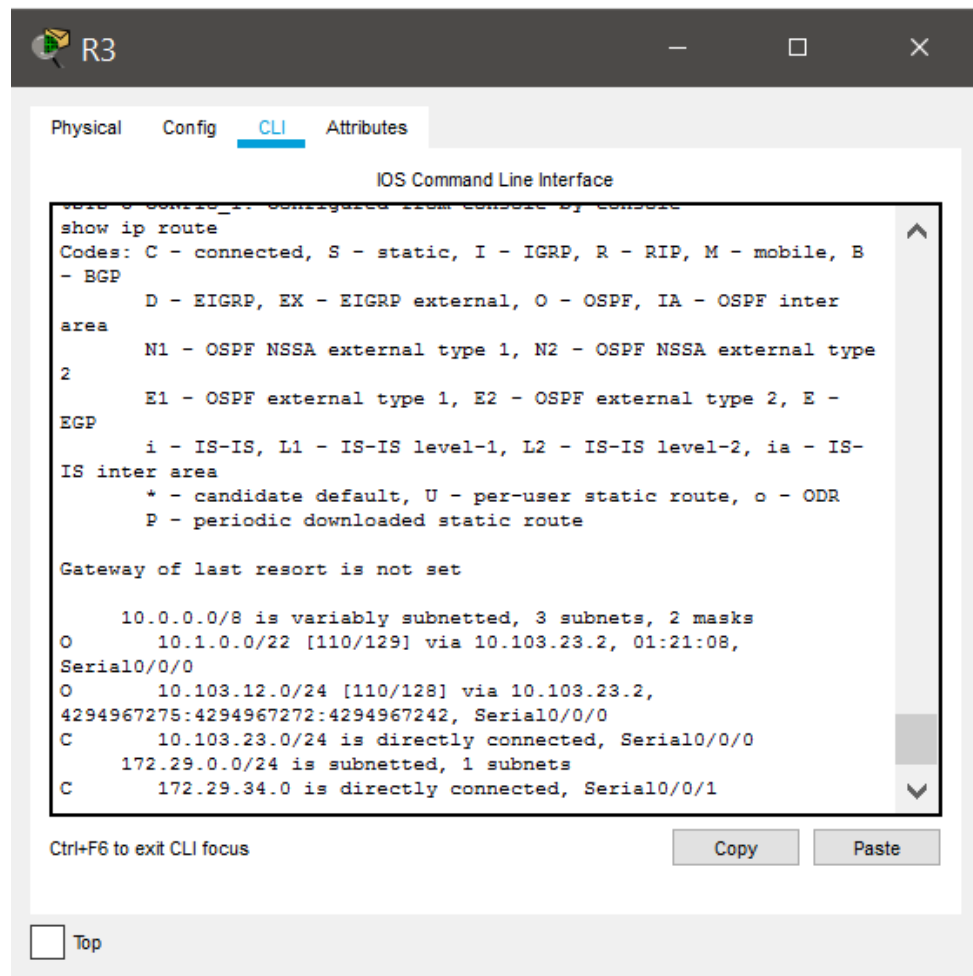
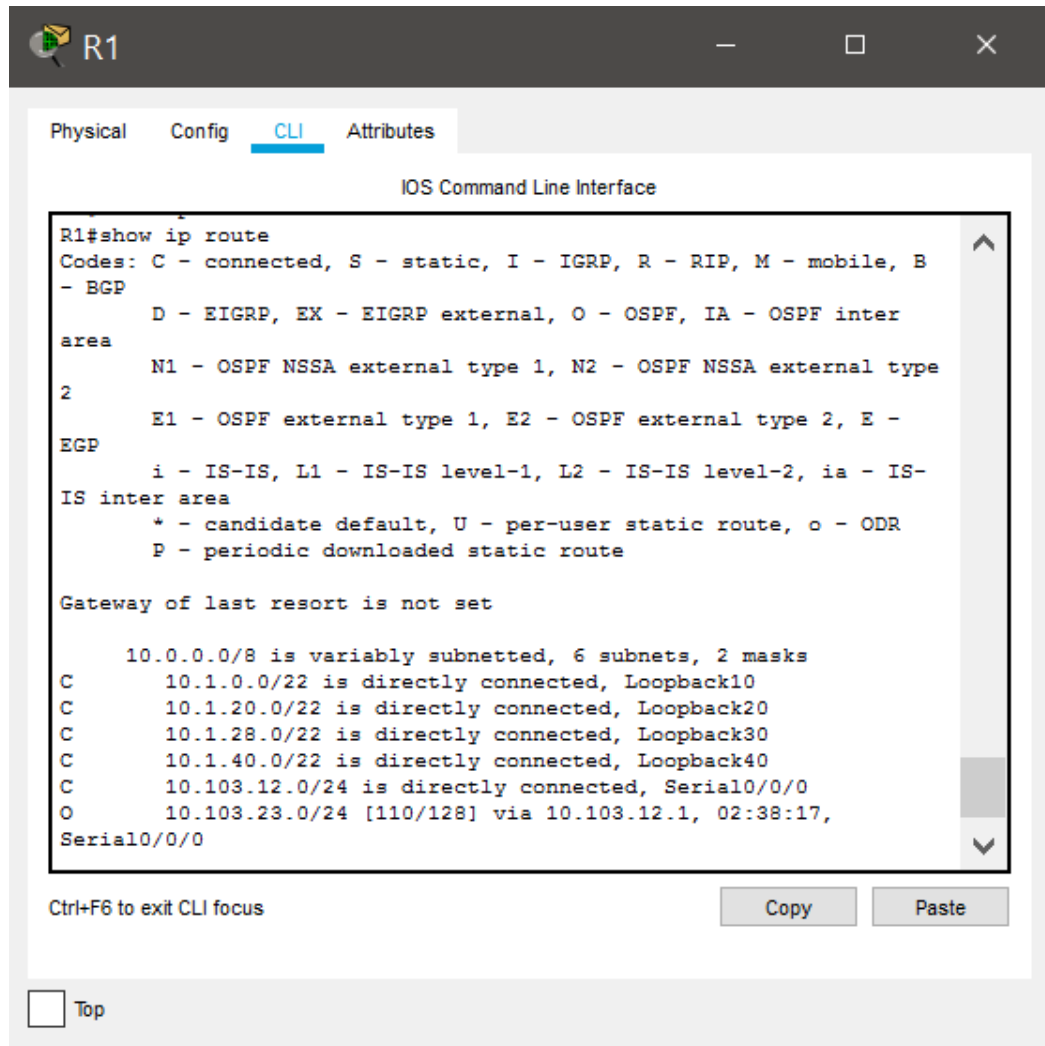


Figura 3 Tabla de enrutamiento R3

6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.1.0.0/22 is directly connected, Loopback10
C       10.1.20.0/22 is directly connected, Loopback20
C       10.1.28.0/22 is directly connected, Loopback30
C       10.1.40.0/22 is directly connected, Loopback40
C       10.103.12.0/24 is directly connected, Serial0/0/0
O       10.103.23.0/24 [110/128] via 10.103.12.1, 02:38:17,
Serial0/0/0
```

*Figura 4*Tabla de enrutamiento R1

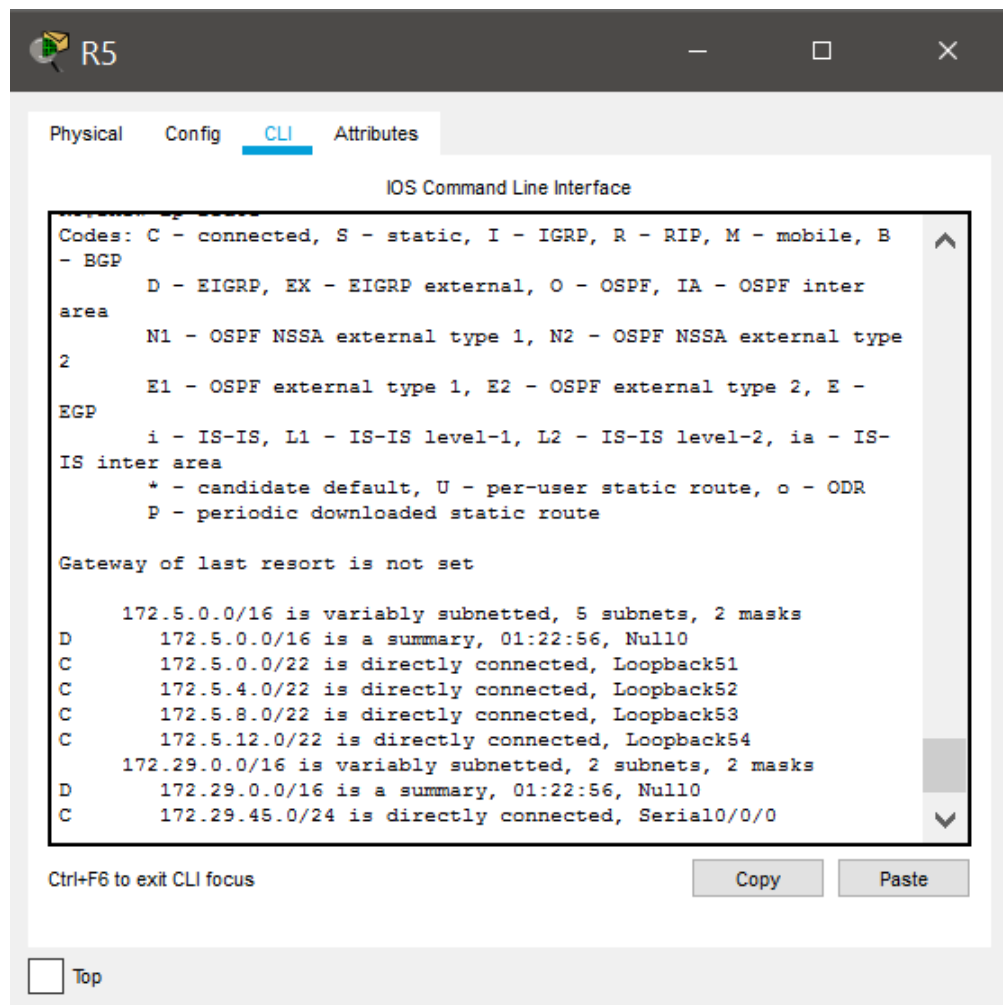


Figura 5 Tabla de enrutamiento R5

ESCENARIO 2

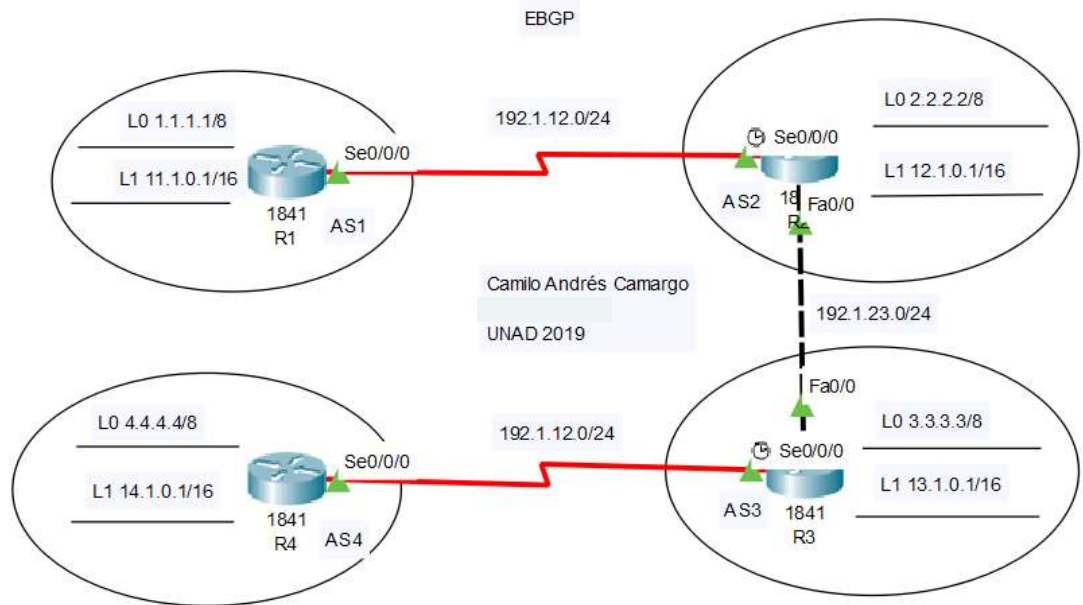


Figura 6 Topología Escenario 2

Información para configuración de los Routers

R1	Interfaz	Dirección IP	Máscara
	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0
R2	Interfaz	Dirección IP	Máscara
	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

R3	Interfaz	Dirección IP	Máscara
	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0

R4	Interfaz	Dirección IP	Máscara
	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Tabla 3 Configuración inicial Escenario 2

Configuración interfaces y loopback R1

```
enable
configure terminal
no ip domain-lookup
hostname R1

interface serial 0/0/0
ip address 192.1.12.1 255.255.255.0
lock rate 64000
no shutdown
exit

interface loopback 0
ip address 1.1.1.1 255.0.0.0

interface loopback 1
ip address 11.1.0.1 255.255.0.0
```


Configuración interfaces y loopback R2.

```
enable
configure terminal
no ip domain-lookup
hostname R2

interface serial 0/0/0
ip address 192.1.12.2 255.255.255.0
no shutdown
exit

interface fastEthernet 0/0
ip address 192.1.23.2 255.255.255.0
no shutdown
exit

interface loopback 0
ip address 2.2.2.2 255.0.0.0

interface loopback 1
ip address 12.1.0.1 255.255.0.0
```

Configuración interfaces y loopback R3.

```
enable
configure terminal
no ip domain-lookup
hostname R2

interface serial 0/0/0
ip address 192.1.34.3 255.255.255.0
no shutdown
exit

interface fastEthernet 0/0
ip address 192.1.23.3 255.255.255.0
no shutdown
exit

interface loopback 0
ip address 3.3.3.3 255.0.0.0
```

```
interface loopback 1
ip address 13.1.0.1 255.255.0.0
```

Configuración interfaces y loopback R4.

```
enable
configure terminal
o ip domain-lookup
hostname R1

interface serial 0/0/0
ip address 192.1.34.4 255.255.255.0
clock rate 64000
no shutdown
exit

interface loopback 0
ip address 4.4.4.4 255.0.0.0

interface loopback 1
ip address 14.1.0.1 255.255.0.0
```

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Configuración de BGP neighbor AS2 en R1

```
router bgp 1
no synchronization
bgp router-id 11.11.11.11
neighbor 192.1.12.2 remote-as 2
network 1.0.0.0 mask 255.0.0.0
network 11.1.0.0 mask 255.255.0.0
```

Configuración de BGP neighbor AS1 en R2

```
router bgp 2
no synchronization
bgp router-id 22.22.22.22
neighbor 192.1.12.1 remote-as 1
network 2.0.0.0 mask 255.0.0.0
network 12.1.0.0 mask 255.255.0.0
```

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Configuración de BGP neighbor AS3 en R2

```
router bgp 2
neighbor 192.1.23.3 remote-as 3
```

Configuración de BGP neighbor y AS2 y 1 en R3

```
router bgp 3
bgp router-id 33.33.33.33
no synchronization
neighbor 192.1.23.2 remote-as 2
network 3.0.0.0 mask 255.0.0.0
network 13.1.0.0 mask 255.255.0.0
```

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 44.44.44.44. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Configuración de BGP neighbor y AS4 en R3

```
router bgp 3
neighbor 192.1.34.4 remote-as 4
```

Configuración de BGP neighbor y AS3 en R4

```
router bgp 4
bgp router-id 44.44.44.44
no synchronization
neighbor 192.1.34.3 remote-as 3
network 4.0.0.0 mask 255.0.0.0
network 14.1.0.0 mask 255.255.0.0
```

```

R1>en
R1#
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B    4.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.12.2, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.12.2, 00:00:00
C    192.1.12.0/24 is directly connected, Serial0/0/0

R1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Figura 7 Tabla de enrutamiento R1

R2

PhysicalConfigCLIAttributes

IOS Command Line Interface

```
R2#sho
R2#show ip ro
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
B    4.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
      12.0.0.0/16 is subnetted, 1 subnets
C        12.1.0.0 is directly connected, Loopback1
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.23.3, 00:00:00
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.23.3, 00:00:00
C    192.1.12.0/24 is directly connected, Serial0/0/0
C    192.1.23.0/24 is directly connected, FastEthernet0/0
```

Ctrl+F6 to exit CLI focusCopyPaste

☐ Top

Figura 8 Tabla de enrutamiento R2

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.34.4, 00:00:00
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial10/0/0

R3#
```

Figura 9 Tabla de enrutamiento R3

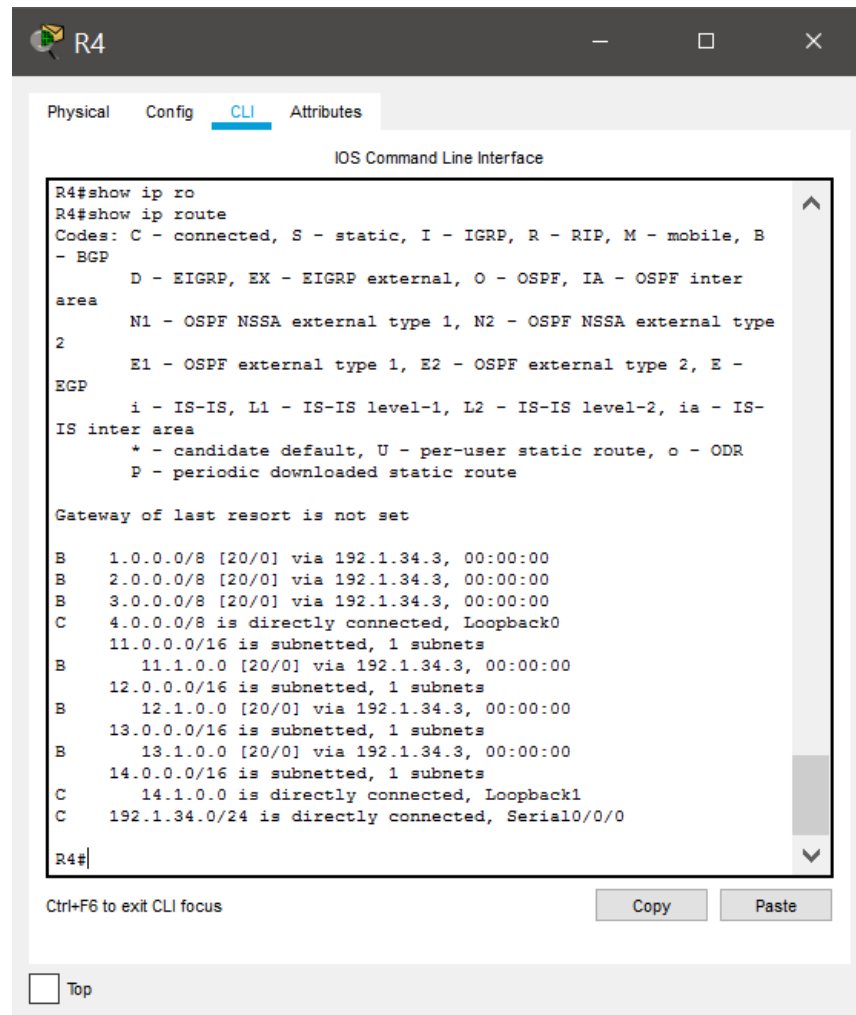


Figura 10 Tabla de enrutamiento R4

ESCENARIO 3

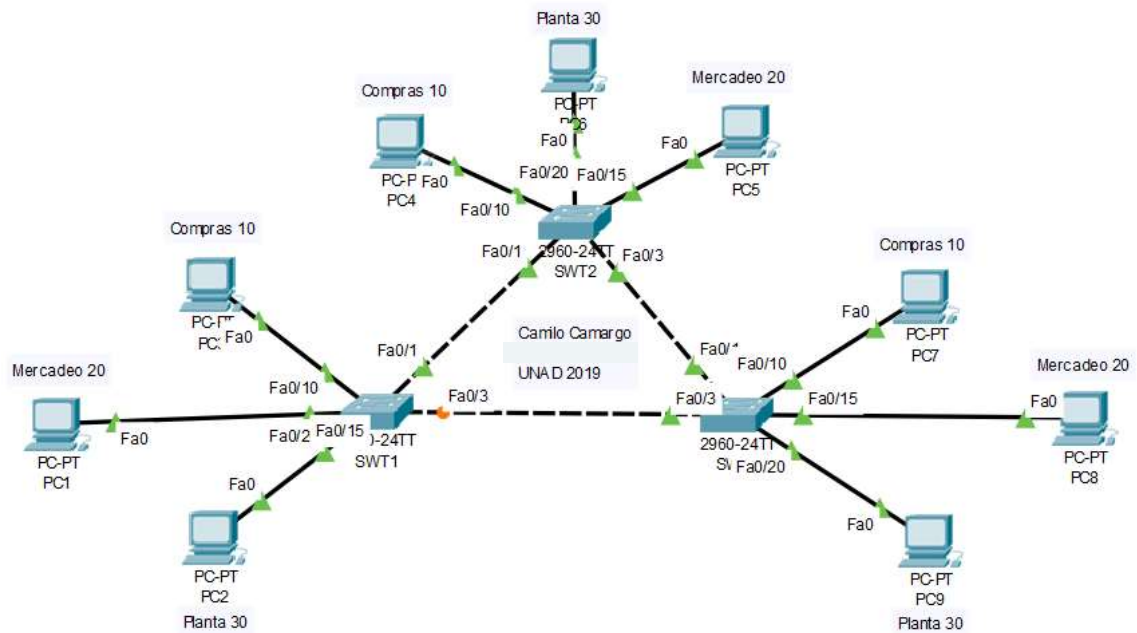


Figura 11 Topología Escenario 3

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW2 se configurará como el servidor. Los switches SW1 y SW3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Configuración VTP en SW1.

```

Enable
configure terminal
hostname SW1
vtp domain CCNP
vtp version 2
vtp mode client
vtp password cisco

```

Configuración VTP en SW2.

```
Enable
configure terminal
hostname SW2
vtp domain CCNP
vtp version 2
vtp mode server
vtp password cisco
```

Configuración VTP en SW3.

```
Enable
configure terminal
hostname SW3
vtp domain CCNP
vtp version 2
vtp mode client
vtp password cisco
```

2. Verifique las configuraciones mediante el comando show vtp status.

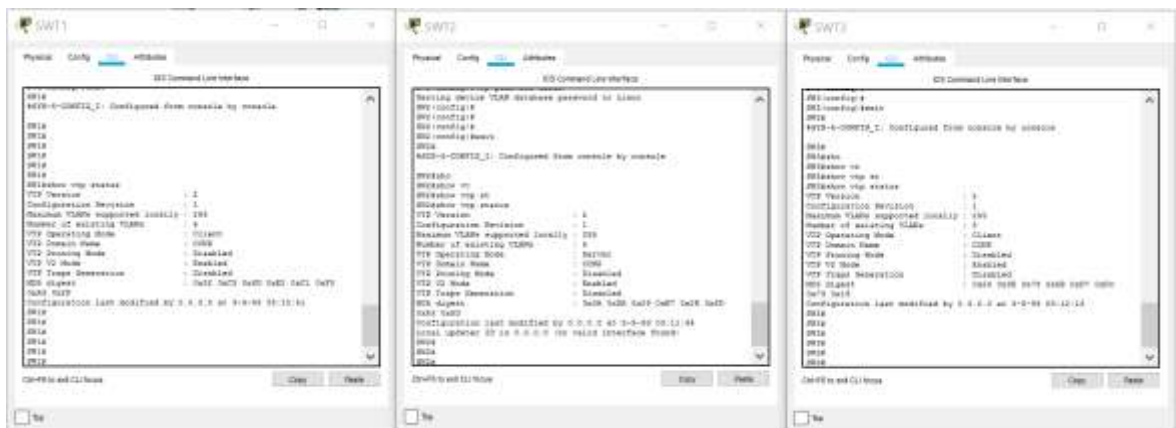


Figura 12 VTP Status

B. Configurar DTP (Dynamic Trunking Protocol).

1. Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Configuración troncal dinámico en SW1.

```
interface FastEthernet0/1
switchport mode dynamic auto
exit
show interfaces trunk
```

Configuración troncal dinámico en SW2.

```
interface FastEthernet0/1
switchport mode dynamic desirable
exit
show interfaces trunk
```

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

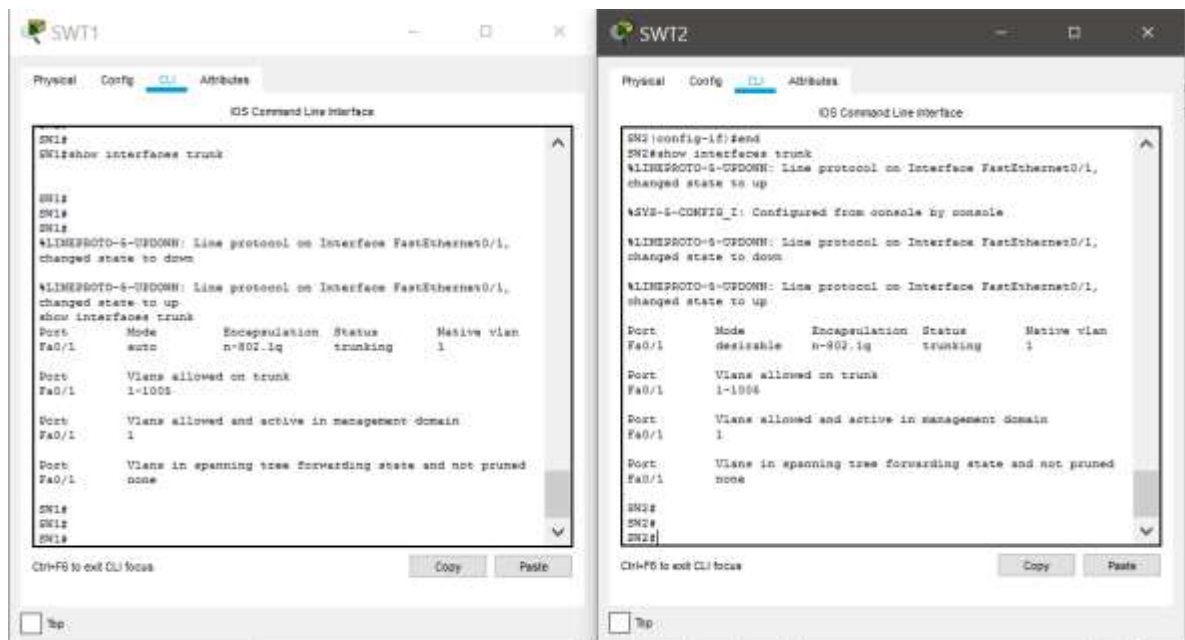


Figura 13 Trunk SW1 y SW2

- Entre SW1 y SW3 configure un enlace "trunk" estático utilizando el comando `switchport mode trunk` en la interfaz F0/3 de SW1

Configuración de Interfaces en SW1.

```
interface FastEthernet0/3
switchport mode trunk
end
show interfaces trunk
```

Configuración de Interfaces en SW3.

```
interface FastEthernet0/3
switchport mode trunk
end
show interfaces trunk
```

4. Verifique el enlace "trunk" el comando show interfaces trunk en SWT1.

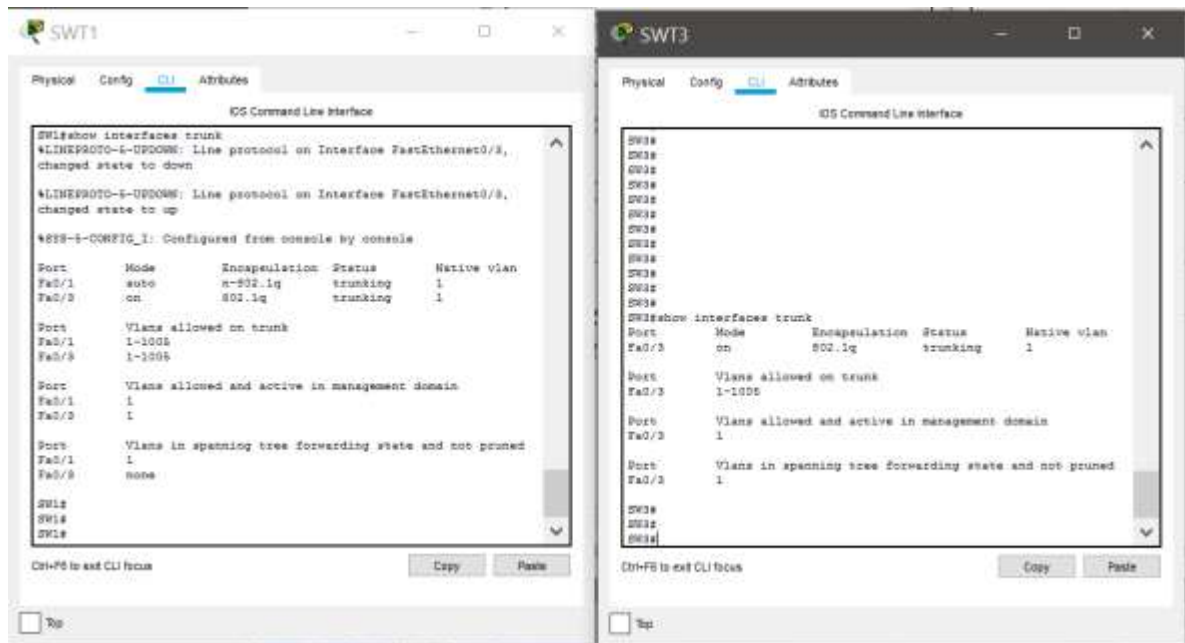


Figura 14 Trunk SWT1 y SWT3

5. Configure un enlace "trunk" permanente entre SWT2 y SWT3.

Configuración de Interfaces en SW2.

```
interface FastEthernet0/3  
switchport mode trunk
```

Configuración de Interfaces en SW3.

```
interface FastEthernet0/1  
switchport mode trunk
```

C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANs Compras (10), Mercadeo (20), Planta (30) y Admon (99)

Configuración de vlans en SW1

```
vlan 10
```

VTP VLAN configuration not allowed when device is in CLIENT mode.

No es posible habilitar la VLAN porque VTP está en modo cliente

Configuración de vlans en SW2

```
vlan 10
```

```
name Compras
```

```
exit
```

```
vlan 20
```

```
name Mercadeo
```

```
exit
```

```
vlan 30
```

```
name Planta
```

```
exit
```

```
vlan 99
```

```
name Admon
```

```
exit
```

2. Verifique que las VLANs han sido agregadas correctamente.

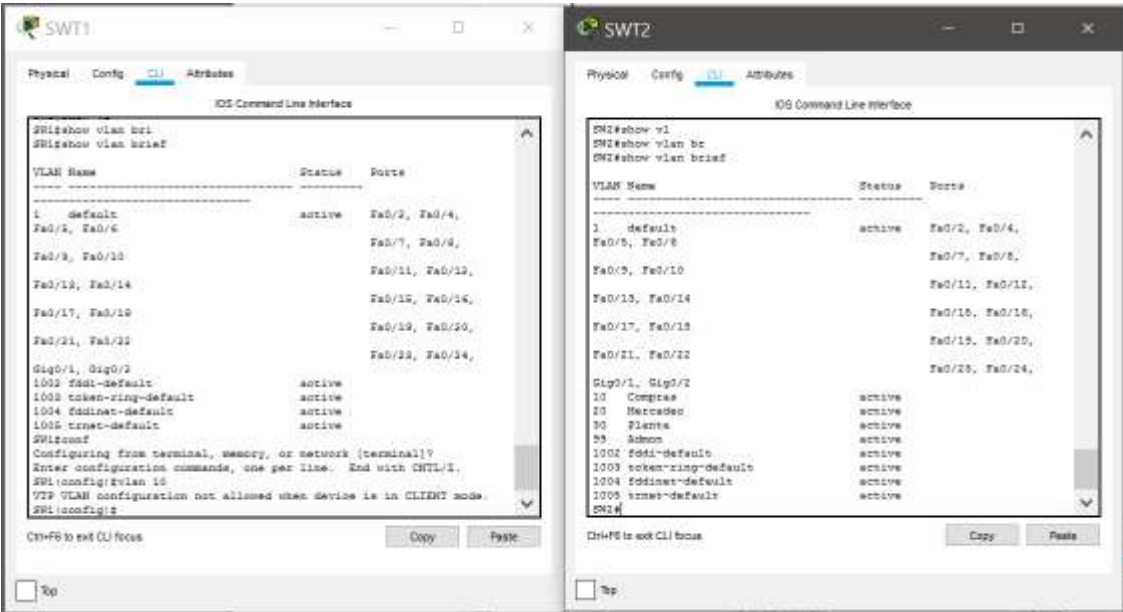


Figura 15 VLANs en SW1 y SW2

3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 20	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

Tabla 4 Interfaces, VLANs, e IP

X = número de cada PC particular

Configuración de VLANs en SWT1.

```
Enable
configure terminal
interface vlan 10
ip address 190.108.10.1 255.255.255.0
exit

interface vlan 20
ip address 190.108.20.1 255.255.255.0
exit

interface vlan 30
ip address 190.108.30.1 255.255.255.0
exit
```

Configuración de VLANs en SWT2.

```
Enable
configure terminal
interface vlan 10
ip address 190.108.10.2 255.255.255.0
exit

interface vlan 20
ip address 190.108.20.2 255.255.255.0
exit

interface vlan 30
ip address 190.108.30.2 255.255.255.0
exit
```

Configuración de VLANs en SWT3

```
Enable
configure terminal
interface vlan 10
ip address 190.108.10.3 255.255.255.0
exit
```



```
interface vlan 20
ip address 190.108.20.3 255.255.255.0
exit
```

```
interface vlan 30
ip address 190.108.30.3 255.255.255.0
exit
```

4. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.

Configuración de F0/10 en SWT1.

```
Enable
configure terminal
interface fastEthernet 0/10
switchport mode access
switchport access vlan 10
end
```

Configuración de F0/10 en SWT2.

```
Enable
configure terminal
interface fastEthernet 0/10
switchport mode access
switchport access vlan 10
end
```

Configuración de F0/10 en SWT3.

```
Enable
configure terminal
interface fastEthernet 0/10
switchport mode access
switchport access vlan 10
end
```

5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

Configuración de F0/15 y F0/20 en SWT1.

```
Enable
configure terminal
interface fastEthernet 0/15
switchport mode access
switchport access vlan 20
exit

interface fastEthernet 0/20
switchport mode access
switchport access vlan 30
end
```

Configuración de F0/15 y F0/20 en SWT2.

```
Enable
configure terminal
interface fa
interface fastEthernet 0/15
switchport mode access
switchport access vlan 20
no shut
exit

interface fastEthernet 0/20
switchport mode access
switchport access vlan 30
end
```

Configuración de F0/15 y F0/20 en SWT3.

```
Enable
configure terminal
interface fastEthernet 0/15
switchport mode access
switchport access vlan 20
exit

interface fastEthernet 0/20
switchport mode access
switchport access vlan 30
end
```

D. Configurar las direcciones IP en los Switches.

En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

Tabla 5 Direcciones SVI VLAN99

Configuración en STW1.

```
interface vlan 99
ip address 190.108.99.1 255.255.255.0
no shutdown
```

Se deshabilitan los puertos que no se están usando

```
interface fastEthernet 0/2
shutdown
exit

interface range fastEthernet 0/4-9
shutdown
exit

interface range fastEthernet 0/11-14
shutdown
exit

interface range fastEthernet 0/16-19
shutdown
exit

interface range fastEthernet 0/21-24
shutdown
```

Configuración en STW2.

```
interface vlan 99
ip address 190.108.99.2 255.255.255.0
no shutdown
```

Se deshabilitan los puertos que no se están usando

```
interface fastEthernet 0/2
shutdown
exit

interface range fastEthernet 0/4-9
shutdown
exit

interface range fastEthernet 0/11-14
shutdown
exit

interface range fastEthernet 0/16-19
shutdown
exit
```

```
interface range fastEthernet 0/21-24
shutdown
```

Configuración en STW3.

```
interface vlan 99
ip address 190.108.99.3 255.255.255.0
no shutdown
```

Se deshabilitan los puertos que no se están usando

```
fastEthernet 0/2
shutdown
exit
```

```
interface range fastEthernet 0/4-9
shutdown
exit
```

```
interface range fastEthernet 0/11-14
shutdown
exit
```

```
interface range fastEthernet 0/16-19
shutdown
exit
```

```
interface range fastEthernet 0/21-24
shutdown
```

E. Verificar la conectividad Extremo a Extremo

1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

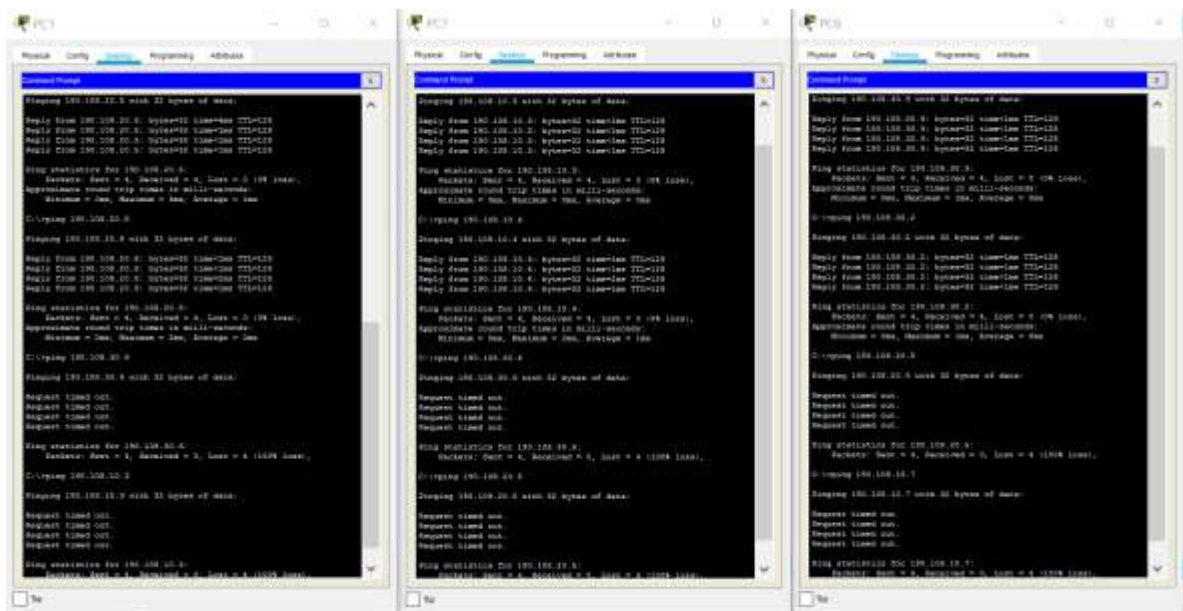


Figura 16 Pruebas de PING en PCs

El ping es exitoso si los equipos están en la misma vlan, es decir, solo hay comunicación entre los 3 equipos de Mercadeo, solo hay comunicación entre los 3 equipos de Planta y solo hay comunicación entre los 3 equipos de Compras. No hay un mecanismo que enrute las 3 Vlan ni los 3 segmentos de red.

2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.



Figura 17 Pruebas de PING en Swithces

El ping entre los tres switch es exitoso evidenciando que la VLAN 99 y las direcciones configuradas en cada son correctas, además todos cuentan con puertos trunk lo que permite el paso de paquetes.

3. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.



Figura 18 Pruebas PING entre Switches y PCs

El ping entre los Switches y los PC no es exitoso debido a que las Vlan Compras, Mercadeo y Planta no tienen una dirección IP asignada como la Vlan99

CONCLUSIONES

Con el desarrollo de esta prueba de habilidades se logró poner en práctica, todo el conocimiento adquirido durante el diplomado y sus laboratorios de Routing y Switching de CCNP y repasar conocimientos básicos en redes aprendidos con anterioridad durante los módulos de CCNA.

En el escenario 1 se hizo un enfoque a Routing, configurando protocolos de enrutamiento avanzados como OSPF y EIGRP en una misma red de acuerdo al requerimiento del caso, e implementando direcciones Loopback y anchos de banda con tiempo de retardo.

En el escenario 2, volvió a hacer énfasis en Routing, esta vez implementando la configuración de vecinos BGP, anuncio de direcciones e identificadores de router (RouterID).

En el escenario 3, se realizó un enfoque a Switching, configurando una red soportada por VLANs con el uso de VTP, optimizando el funcionamiento de la red y su seguridad, dividiendo el tráfico para cada área de la empresa, una muy buena solución en infraestructura que no cuentan con la capacidad de comprar e implementar Routers y sus protocolo de enrutamiento.

REFERENCIAS

- Cisco systems - guía de diseño de ospf - recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.pdf
- Cisco systems - introducción a eigrp - recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.pdf
- Cisco systems - redistribución de protocolos de ruteo - recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.pdf
- Cisco systems - casos prácticos de bgp - recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.pdf
- Cisco systems - cómo comprender vlan trunk protocol (vtp) - recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf
- Cisco systems - configurando el vlan trunk protocol (vtp) - recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/98154-conf-vlan.pdf